

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (Agreement) supplements and is incorporated into the existing Underlying Contract (Contract) known as the **[Insert Contract Title]** covering the provision of **[Insert Description of Contracted Services]** entered into by and between **[Insert Legal Name of Business Associate]** (Business Associate) and **[Insert Legal Name of Covered Entity]** (Covered Entity) on **[Insert Agreement Signed Date]**. This Agreement is effective beginning on **[Insert Agreement Effective Date]** and terminates any prior existing Agreements.

This Agreement is specific to those services, activities, or functions covered in the Contract where it has been determined that the Business Associate is performing services, activities, or functions on behalf of the Covered Entity that are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These services, activities, or functions include:

### **[INSERT DESCRIPTION OF SERVICES, ACTIVITIES OR FUNCTIONS CONTRACTED FOR]**

The Covered Entity and Business Associate agree to modify the Contract to incorporate the terms of this Agreement and to comply with the requirements of HIPAA addressing confidentiality, security and the transmission of individually identifiable health information created, used or maintained by the Business Associate during the performance of the Contract and after the Contract is terminated. The Business Associate agrees that any conflict between provisions of the Contract and the Agreement will be governed by the terms of the Agreement.

## **1. DEFINITIONS**

***Protected Health Information (PHI)*** means:

Health information, including demographic information, created, received, maintained, or transmitted by the Business Associate, on behalf of the Covered Entity, where such information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual, that identifies the individual or provides a reasonable basis to believe that it can be used to identify an individual.

PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA) (*see* 20 U.S.C. 1232g, *et. seq.*) and employment records held by the Covered Entity in its role as employer.

***Individual*** means:

The person who is the subject of protected health information or the personal representative of an Individual as defined and provided for under applicable provisions of HIPAA.

***Disclosure*** means:

The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

***Designated Record Set*** means:

- (1) A group of records maintained by or for a covered entity that is:
  - (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
  - (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

(iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) For purposes of this Agreement, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

## **2. PROHIBITION ON UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION**

The Business Associate shall not use or disclose any PHI except as permitted or required by the Contract or this Agreement, as permitted or required by law, or as otherwise authorized in writing by the Covered Entity.

## **3. PERMITTED USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION**

The Business Associate may use or disclose PHI only for the following purpose(s):

- a. for the delivery of the services, program management, activities, or functions contracted for in the Contract; or
- b. for meeting contractual or legal obligations as established in any agreements between the parties evidencing their business relationship; or
- c. as permitted by HIPAA if such use or disclosure were made by the Covered Entity or otherwise required by applicable law, rule or regulation; or
- d. for use in the operations of the Business Associate as provided in paragraph 4 of this Agreement; or
- e. as otherwise authorized by the Covered Entity in writing; or
- f. data aggregation for the health care operations of the Covered Entity.

## **4. USE OF PROTECTED HEALTH INFORMATION IN BUSINESS ASSOCIATE OPERATIONS**

The Business Associate may use or disclose PHI as necessary for the delivery of the services or programs provided for in the Agreement, including appropriate management and administration of programs or services, or to fulfill the contractual or legal obligations of the Business Associate provided:

- a. the disclosure is permitted or required by law; or
- b. the Business Associate obtains reasonable assurances, evidenced by a written contract, from any person or organization to which the Business Associate will disclose PHI that such person or organization shall:
  - (i) hold all PHI in confidence and use or further disclose it only for the purpose for which the Business Associate disclosed it to the person or organization, or as required by law; and
  - (ii) notify the Business Associate, who will in turn promptly notify the Covered Entity, of any instance that the person or organization becomes aware of in which PHI was improperly disclosed.

## **5. SAFEGUARDING AND MAINTENANCE OF PROTECTED HEALTH INFORMATION**

- a. The Business Associate will develop, implement, maintain, and use:
  - (i) appropriate administrative, technical, and physical safeguards to prevent improper use or disclosure of PHI, in any form or media; and
  - (ii) appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity and availability of electronically maintained or transmitted PHI.
- b. The Business Associate will document and keep these safeguards and security measures current and available for inspection by the Covered Entity or its agents, upon request. Security measures employed by the Business Associate must comply with HIPAA security requirements on or before the date such requirements become effective.

## **6. USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION BY SUBCONTRACTORS AND AGENTS OF THE BUSINESS ASSOCIATE**

The Business Associate agrees to require any agent, including subcontractors, to whom the Business Associate provides PHI to comply with the same restrictions and conditions applicable to the Business Associate with respect to PHI. This provision does not apply to the use or disclosure of PHI by subcontractors that provide health care treatment to individuals or to other persons or organizations that have entered into an Organized Health Care Arrangement (OHCA) as provided for under the provisions of HIPAA.

## **7. COMPLIANCE WITH ELECTRONIC TRANSACTIONS AND CODE SET REGULATIONS**

If the Business Associate conducts any HIPAA-covered standard electronic transaction(s) on behalf of the Covered Entity, the Business Associate will comply with the applicable provisions of HIPAA for such standard transaction(s). The Business Associate will likewise require any subcontractor or agent conducting any standard electronic transaction(s) on behalf of the Business Associate, for services or programs covered by the Contract, to comply with the applicable provisions of HIPAA relating to standard transactions.

- a. General requirements.
  - (i) If any entity requests the Business Associate to conduct any of the standard electronic transactions, the Business Associate must comply with the request.
  - (ii) The Business Associate may not delay or reject a transaction, or otherwise adversely affect or impact the other entity or the transaction submitted, because the transaction is a standard electronic transaction.
  - (iii) The Business Associate may not reject a standard electronic transaction on the basis that it contains data elements not needed or used by the Business Associate (e.g., coordination of benefits information).
  - (iv) The Business Associate may not offer an incentive to a health care provider to conduct a covered transaction through direct data entry (as described in CFR 45 §162.923(b)) rather than as a standard electronic transaction.
  - (v) Business Associates operating as a health care clearinghouse, or requiring an entity to use a health care clearinghouse to receive, process, or transmit standard electronic transactions may not charge fees or impose costs in excess of the fees or costs for normal telecommunications that the entity incurs when it directly transmits, or receives, a standard electronic transaction to, or from, the Business Associate.
- b. The Business Associate will not enter into, or permit its subcontractors or agents to enter into, any agreement related to the conducting of standard electronic transactions for or on behalf of the Covered Entity that:
  - (i) changes or modifies the definition, data condition, or use of a data element or segment in an implementation specification; or
  - (ii) adds any data elements or segments to the maximum defined data set; or
  - (iii) uses any code or data elements that are marked “not used” in the implementation specification or are not contained within the implementation specification; or
  - (iv) changes the meaning or intent of any implementations specification.
- c. If the Business Associate receives a standard electronic transaction and coordinates benefits with another health plan, it must store the coordination of benefits data it needs to forward the standard electronic transaction to the other health plan.

## **8. ACCESS TO PROTECTED HEALTH INFORMATION**

At the request of the Covered Entity, the Business Associate agrees to provide access to PHI held by the Business Associate that the Covered Entity has determined to be part of the Designated Record Sets of the programs covered by the Agreement. Access to PHI will be provided to the Covered Entity or to an Individual as directed by the Covered Entity to comply with applicable HIPAA requirements. The Covered Entity may

delegate responsibility for the performance of all legal obligations, including HIPAA rights, relating to the Designated Record Set to the Business Associate.

#### **9. AMENDMENT OR CORRECTION TO PROTECTED HEALTH INFORMATION**

At the direction of the Covered Entity, the Business Associate agrees to amend or correct PHI that the Covered Entity determines is included in the Designated Record Set held by the Business Associate. The Business Associate agrees that any amendment or correction will be completed by the Business Associate in accordance with applicable HIPAA provisions.

#### **10. REPORTING OF UNAUTHORIZED USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION**

The Business Associate will inform the Covered Entity of any use or disclosure of PHI not authorized by this Agreement or in writing by the Covered Entity within **[Insert Number of Days]** business days of becoming aware of such use or disclosure. The Covered Entity, at its discretion, may require a written report. If a written report is requested by the Covered Entity, the Business Associate agrees to forward a written report to the Covered Entity not more than **[Insert Number of Days]** business days after such request is made. Written and verbal reports of unauthorized use or disclosure will include:

- a. A description of the circumstances of the unauthorized use or disclosure;
- b. the PHI used or disclosed;
- c. the person or persons making the unauthorized disclosure;
- d. the person, persons or organization that received the unauthorized disclosure;
- e. what actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the unauthorized use or disclosure; and
- f. the actions the Business Associate has taken or will take to prevent future similar unauthorized uses or disclosures.

#### **11. MITIGATING EFFECT OF UNAUTHORIZED DISCLOSURES OR MISUSE OF PROTECTED HEALTH INFORMATION**

The Business Associate agrees to mitigate, to the extent practicable, any harmful effect known to the Business Associate created by an improper use or disclosure of PHI by the Business Associate in violation of the requirements of this Agreement.

#### **12. TRACKING AND ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE**

- a. The Business Associate agrees to track disclosures of PHI as required by the applicable provisions of HIPAA. Specifically, the Business Associate agrees that it will maintain a record of all PHI disclosures made to third parties. The Business Associate agrees that the following information will be recorded:
  - (i) the date the PHI was disclosed;
  - (ii) the name and address, if known, of the person or entity that the PHI was disclosed to;
  - (iii) a brief description of the PHI disclosed; and
  - (iv) a brief statement describing the purpose for the disclosure.
- b. For repetitive disclosures that the Business Associate makes to the same person or entity for a single purpose, the Business Associate will provide:
  - (i) the disclosure information as specified in Paragraph 12(a)(i-iv) of this Agreement for the first of such repetitive disclosures;
  - (ii) the frequency, periodicity or number of such repetitive disclosures; and
  - (iii) the date of the most recent of such repetitive disclosures.
- c. The Business Associate will make the record of disclosures available to the Covered Entity within **[Insert Number of Days]** business days after receiving a request by the Covered Entity.

d. Exceptions from Disclosure Tracking.

The Business Associate is not required to track or record disclosures of PHI, or to provide an accounting of disclosures for PHI meeting the following conditions:

- (i) disclosures of PHI that are permitted under this Agreement, or otherwise expressly authorized by the Covered Entity in writing; and
- (ii) disclosures of PHI for the following:
  - (1) for purposes of treatment, payment or health care operations activity of the Covered Entity;
  - (2) in response to a request from an Individual who is the subject of the disclosed PHI, or to that Individual's Personal Representative;
  - (3) made to persons involved in health care or payment for health care of the Individual;
  - (4) for disaster relief notification purposes;
  - (5) for national security or intelligence purposes; or,
  - (6) to law enforcement officials or correctional institutions regarding Individuals in custodial situations.

e. Disclosure Tracking Time Periods.

Business Associate agrees to maintain and make available to the Covered Entity upon its request information on disclosures of PHI made by the Business Associate for the six-year period preceding the request, but not including disclosures made prior to April 14, 2003, or the date that the Business Associate began performing covered services, activities, or functions on behalf of the Covered Entity, whichever is later.

### 13. ACCOUNTING TO THE COVERED ENTITY AND TO GOVERNMENT AGENCIES

The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Covered Entity, or to the Secretary of Health and Human Services (HHS) in a time and manner determined by the Covered Entity or the Secretary or designee, for purposes of determining compliance by the Covered Entity with the requirements of HIPAA. Further, the Business Associate agrees to promptly notify the Covered Entity of communications with HHS regarding PHI and will provide the Covered Entity with copies of any PHI or other information the Business Associate has made available to HHS under this provision.

### 14. TERM AND TERMINATION OF AGREEMENT

- a. The Business Associate and Covered Entity agree that this Agreement becomes effective on **[Insert Effective Date]**.
- b. The Business Associate agrees that if in good faith the Covered Entity determines that the Business Associate has materially breached any of its obligations under this Agreement, the Covered Entity at its discretion, has the right to:
  - (i) exercise any of its rights to reports, access and inspection under this Agreement, and, or
  - (ii) require the Business Associate to submit to a plan of monitoring and reporting, as the Covered Entity determines necessary to maintain compliance with this Agreement; and, or
  - (iii) provide the Business Associate with a defined time period to cure the breach; or
  - (iv) terminate the Agreement in accordance with applicable state statutes.
- c. Before exercising any of these options, the Covered Entity will provide written notice of preliminary determination to the Business Associate describing the violation and the action the Covered Entity intends to take.

### 15. RETURN OR DESTRUCTION OF PHI

Upon termination, cancellation, expiration or other conclusion of this Agreement, the Business Associate will:

- a. Return to the Covered Entity or, if return is not feasible, destroy all PHI and any compilation of PHI in any media or form. The Business Associate agrees to ensure that this provision also applies to PHI in possession of subcontractors or agents of the Business Associate provided to the agent or

subcontractor by the Business Associate. The Business Associate agrees that any original record or copy of PHI in any media is included in this provision as are any original or copy of PHI provided to subcontractors or agents of the Business Associate by the Business Associate. The Business Associate agrees to complete the return or destruction as promptly as possible, but not more than **[Insert Number of Days]** business days after the effective date of termination of this Agreement. The Business Associate will provide written documentation evidencing that return or destruction of all PHI has been completed.

- b. If the Business Associate believes that the return or destruction of PHI is not feasible, the Business Associate shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Business Associate and Covered Entity that return or destruction is not feasible, The Business Associate shall extend the protections of this Agreement to PHI and prohibit further uses or disclosures of the PHI of the Covered Entity without express written authorization of the Covered Entity. Subsequent use or disclosure of any PHI subject to this provision will be limited to the use or disclosure that makes return or destruction unfeasible.

#### **16. MISCELLANEOUS**

- a. Automatic Amendment: This Agreement shall automatically incorporate any change or modification to HIPAA as of the effective date of the change or modification. The Business Associate agrees to maintain compliance with all changes or modifications to HIPAA as required.
- b. Interpretation of Terms or Conditions of Agreement: Any ambiguity in this Agreement shall be construed and resolved in favor of a meaning that permits the Covered Entity and Business Associate to comply with HIPAA.
- c. Submission of Compliance Plan: The Business Associate agrees that a HIPAA compliance plan may be requested by the Covered Entity. If requested by the Covered Entity, the Business Associate agrees to provide periodic reports of the progress of the compliance plan. Further, the Business Associate agrees that the plan and progress reports will comply with the requirements of the Covered Entity.

**IN WITNESS WHEREOF**, the undersigned have caused this Agreement to be duly executed by their respective representatives.

#### **COVERED ENTITY**

#### **BUSINESS ASSOCIATE**

**By:** \_\_\_\_\_

**By:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Date:** \_\_\_\_\_